OnGo Private LTE Deployment Guide

September 2020

CONTENTS

CONTENTS

Introduction

Overview

This paper is a guide for deploying Private LTE networks using OnGo's LTE in the CBRS band. It provides a walk-through of the deployment process and examines the major choices involved.

Who Should Read this Guide?

With the opening up of the CBRS band to the public, the FCC removed several key barriers to deploying small-scale LTE networks. It is now possible to deploy private LTE networks much more quickly and at a much lower cost than ever.

We have written this guide for enterprises and other organizations interested in building a private OnGo-based LTE network to meet their business needs. We intend that company leaders learn the current "art of the possible," while also helping network engineers ask the right questions when planning a private, broadband, wireless network deployment.

Much of the design, deployment, and operational tasks described in this paper can be addressed in detail by an OnGo system service provider – many of whom belong to the CBRS Alliance. Understanding the scope of services, and the nature of the various tasks involved, will help the reader define their service needs and select an appropriate service provider.

Who's Who in OnGo

OnGo is the result of work by many organizations:

- The FCC – The Federal Communications Commission defined the part 96 regulations that opened access to the CBRS band.
- WInnForum – The Wireless Innovation Forum defined the requirements for CBRS- compliant physical devices.
- CBRS Alliance – The CBRS Alliance defines the requirements for OnGo technologies in the 3.5 GHz band and certifies OnGo-compliant equipment.
- 3GPP – The 3GPP standards body represents the community of 3GPP equipment manufacturers and service providers in order to establish the LTE and 5G standards.

CBRS Overview

Wireless communication has become the "fourth utility." For most organizations it has become as essential as power, water, and Internet connectivity for doing business. While demand for mobile communication appears limitless, unfortunately wireless spectrum—the medium for carrying wireless information—is finite, and increasingly scarce and valuable.

Introduction

To address current and future needs for wireless spectrum, in April 2015 the Federal Communications Commission (FCC) formally established the Citizen Broadband Radio Service (CBRS). Previously reserved solely for military and other government-approved uses, CBRS opens up 150 MHz of spectrum in the 3.5 GHz band so that private organizations may share this spectrum with incumbent users. The CBRS Alliance created OnGo to promote the use of LTE in the 3.5 GHz band, although other technologies can also make use of the band. The FCC partitioned 150 MHz of the 3.5 GHz band into 15 x 10 MHz channels. Access to the channels is dynamic and controlled by dedicated spectrum-management services known as Spectrum Access Systems (SAS).

PAL vs GAA

Users who operate in the CBRS band have different priority levels. Top priority lies with the Tier 1 incumbent users such as the federal government, fixed satellite users, and grandfathered wireless users. Next in priority are Tier 2, or Priority Access License (PAL), users. These are licensed users who acquire spectrum licenses through an FCC auction. PAL users must not cause harmful interference to Tier 1 users. Third priority is given to Tier 3 General Authorized Access (GAA) users who deploy "lightly-licensed" devices. GAA users must not cause harmful interference to the higher-tier users.

The FCC auctions PALs on a per-county basis, with sublicensing permitted. Of the 15 channels in the CBRS band, the FCC allocates seven for PAL licensees. Any spectrum not used by PAL holders or the protected incumbents can be used by GAA users. Currently, GAA users are not afforded interference protection from each other.

CBSDs

Access Points are termed Citizens Broadband Radio Service Devices (CBSDs) in CBRS. CBSDs come in many types – fully integrated Smallcells, Distributed Radio Heads, or Antenna Clusters. CBRS defines a CBSD as a logical entity that radiates RF power, has antenna characteristics and is geolocated. CBSDs come in two classes, defined by their output power, and therefore range: Category A devices, emit less than one watt of power; Category B devices, typically for outdoor use, emit up to 50 watts. In an OnGo network, the LTE eNodeBs (base stations) are connected to CBSDs.

Device Type	Maximum EIRP (dBm/10 MHz)	Limitations
Category A CBSD	30 (1W)	• Outdoor antenna height limited to 6 meters Height Above Average Terrain (HAAT). • If operation exceeds antenna height or max Category A power limits, the device is subject to Category B limitations.
Category B CBSD	47 (50W)	• Limited to outdoor operation. • Must be professionally installed.

EUDs

In CBRS, End User Devices (EUDs) are the user-facing element. These devices can be either mobile or fixed and must be limited in power to < 23 dBm/10 MHz (<200 mW). EUDs may operate only if given permission by a CBSD. In an OnGo network, the EUDs are generally LTE User Equipment (UE) devices.

SAS

All CBSDs must register with an FCC-certified Spectrum Access System (SAS) and obtain a channel grant from the SAS before beginning transmission in the CBRS band. The SAS allocates spectrum to individual CBSDs to prevent interference with incumbent systems and PAL license holders. To coordinate the CBRS band's usage, the SAS maintains a database of CBSDs and incumbent devices to calculate aggregate interference. In order for a SAS to grant access to channels in the lower 100 MHz of the CBRS band, the SAS must have access to Environmental Sensing Capability (ESC). The ESC is a network of sensors used to detect federal frequency use in the 3550–3650 MHz band where U.S. Navy radar systems can operate, primarily along the Pacific, Atlantic and Gulf coasts. The ESC informs the SAS of radar operation so that the SAS can prevent any CBRS interference with naval operations. The SAS uses propagation models to predict potential interference with incumbent systems and transmits operating parameters to CBSDs so as to avoid potential interference. A new CBSD requests access to a range of frequencies from the SAS, and, based on the location of the CBSD, its category, and its antenna characteristics, the SAS grants access to one or more CBRS channels. When higher-priority users need channel access, the SAS can instruct the CBSDs to reduce their output power, stop using currently allocated channels, or shut off entirely to avoid interference with PAL users or incumbent systems.

Introduction

Several FCC-certified SAS systems have been deployed across the country and are operated by various companies that share information among each other. Before a CBRS user deploys a CBSD, they need to subscribe to a SAS service from an FCC-certified SAS administrator. Under Part 96 rules, a SAS does not guarantee interference protection among GAA users. However, WInnForum and other CBRS Alliance standards bodies have come together to develop a framework called Coexistence for GAA users, to help manage GAA operation.

CPIs

CBSDs must be registered by a Certified Professional Installer (CPI) who maintains information about the CBSD as well as provides its detailed location information to the SASs. The FCC does not require that CBSDs be installed by a CPI, but each new CBSD must be registered by a CPI with the SAS. CPIs are certified by one of the Training Program Administrators (TPAs) approved by WInnForum.

Gathering Requirements

The first step in any successful deployment requires a detailed understanding of your organization's needs as well as the problems you wish to solve with an OnGo private LTE network. By starting with identifying your critical use cases, your networking team—or an OnGo service provider—can design a system to meet your needs.

Understanding Needs, Use Cases, and Problems to be Solved

The first step in gathering requirements is to identify the critical use-cases for your OnGo Private LTE network. Here we provide a list of questions you should consider when defining your network requirements:

- What is the primary purpose of your Private LTE network?
  - For example, will the network need to provide data connectivity for IoT devices, or will it be used exclusively for mobile phones? If for mobile phones, will your mobile devices also require support for data? The answers to these initial questions will drive many decisions and provide the answers to the more detailed questions below.
- Who will be connecting to your Private LTE network?
  - Should access to the network be limited to a static list of users? Employees of your organization only? Or will visitors, external partners, or guests also require access to the network?
  - Will users require privileged access to critical business assets? Will users be members of particular groups requiring constant wireless connectivity, such as executive leadership, IT, security, or development? Understanding roles and access privileges will ensure proper authentication and security, as well as your device and user-provisioning needs.
- What will be connecting to your network?
  - This can include gateways, internal communication channels, and applications, as well as IoT devices, cameras, and various mobile user devices.
  - If you have existing devices that you want to connect via your private LTE network, what interfaces do they have?

Gathering Requirements

- What level of security do you need?
  - To supply enterprise-grade LTE security (e.g., device authentication, traffic encryption), an OnGo network requires little to no extra work. If you need additional protection, you should define your security requirements as early as possible.
- Are the devices connecting to your network going to be mobile or fixed-in-place?
  - Fixed and mobile devices have different network architectures and device-management requirements.
- How many users, devices, or IoT nodes will access the network?
  - Depending on whether you need to support hundreds or thousands of connections, scoping the network correctly will be crucial to achieving the required performance.
- What type of traffic will those users and devices be generating?
  - For example, the data requirements of security cameras streaming high-definition video are very different from a device periodically providing status updates.
- What will the devices be connecting to?
  - If devices and users need to connect to other company networks or the Internet at large, you need to make provisions for backhaul communications. However, backhaul support may be unnecessary if the devices will be sending data only among each other.
- Will mobility into and out of the network be needed?
  - If needed, you can configure your Private LTE network to allow devices to roam seamlessly into and out of the network. Arrangements must be made with existing network operators to support roaming to and from their systems.
- In what type of environment will the system be deployed?
  - Given that OnGo Private LTE networks function both indoors and outdoors, your specific environment will determine many aspects of your system.

- What wireless data infrastructure do you already have?
  - If you have an existing WiFi network, you can allocate devices and data traffic to the system that best supports your needs. This can improve the performance of both networks.
- How mission-critical is your network?
  - The CBRS band provides multiple levels of licensing, with licensed users having priority when allocating channels. If your deployment requires high availability, you may need to engage the services of a provider with a PAL license.
- What growth do you anticipate over the next one-to-three years?
  - If you expect to add more users, nodes, functionality, or sites, you should plan your deployment accordingly.
- What kind of infrastructure deployment approach do you prefer for the Network and Management elements: on-premise, cloud, hybrid cloud?
  - If you already have on-premise hosting options, hosting locally may make sense. If preferred, some or all of the network elements may reside in the cloud.
- How do you want to install, operate, and own the network?
  - For example, does your organization prefer to capitalize some or all of the equipment? Or do you prefer to subscribe to services? Will your internal team manage the core network, or do you desire a managed services option? OnGo deployments provide the flexibility to match service deployment with your business model.

This guide will take you through the different deployment processes for two separate sites, each with very distinct requirements. Scenario A is a typical new building deployment. Scenario B is for a larger and more complex sports venue. By going through the detailed deployment process of each, we hope to give you clear examples to help guide the planning of your network.

Scenario A: Smart-Building Network Requirements

For our first scenario, we will look at the requirements for an OnGo-based network supporting the needs of a standard office building. Like any new building today, this facility will require several smart devices to monitor the building, specifically various support systems within the building that control security, HVAC, and lighting, among others. In addition, staff members require access to data while working throughout the building. Most devices remain fixed-in-place, with locations known at the time of installation. Employees do not require seamless mobility, and an IT Team will provision devices manually, so dynamic provisioning is not needed. Most sensors and controls have low bandwidth requirements, except for the security cameras, which consume high uplink bandwidth. The total number of sensors is approximately 500, with 10–20 security cameras. Most of the smart devices will be inside the building, with a few around the exterior perimeter of the building. Security is critical, but the system is not genuinely mission-critical – disruption of the network will not render the building unusable.

Figure 1.

Scenario B: Sports Venue Requirements

In the second scenario, we will detail the deployment of an OnGo network at a stadium or sports complex, intended to support large event operations. The primary use case is to provide voice and data to staff during events, when the public networks may be saturated. In addition, the network must support a small number of mobile high-definition video feeds from moving camera crews. Since the venue is large and the staff will be moving around the site during the event, the network must support seamless mobility. The total number of staff during games could reach as many as 200 people. Also, teams and coaches will need network access during events. While security is not a top concern, high-availability is. The cost of network failure could harm the reputation of the facility owner and jeopardize future revenue opportunities.

Figure 2.

Survey & Planning

Once you have determined your primary use cases and requirements, the next step is to begin planning your deployment.

Site Survey

To begin, you will need to survey the area you intend your network to cover. You must determine how many CBSDs will be required, along with their location. The frequency band in which CBSDs operate (3.5 GHz) does not propagate in the same way as "regular" LTE signals and operates at a lower power level (<50 watts) than a macro LTE cell. While the actual list of information required to plan a full deployment may be longer, here we provide some examples of the type of information needed:

- The overall dimensions of the area to be covered (length, width, height, area usage type, etc.).
- Dimensions of the outdoor coverage areas.
- Dimensions of the indoor coverage areas.
- Wall dimensions and construction types (concrete, wood, metal studs, etc.).
- Location and dimensions of structures in the area of coverage (large pieces of furniture, large objects, obstructions, construction materials, etc.).
- Locations of power and data sources, as well as inaccessible areas. Note: If WiFi infrastructure already exists, you can use the WiFi Access Points as a simple way to map out convenient locations for CBSDs.
- Areas of potential interference (incumbents, radars, cell towers, etc.).
- The current and expected device and subscriber density. This should include an understanding of the expected end uses, such as IoT device types, Mobile Users, etc.
- Location and availability for on-site infrastructure elements as required (data center, networking elements, network management systems, controllers, etc.).
- Location and interfaces (wired and wireless) of any existing devices that will connect to your network.

The intent of these questions is to scope out the overall scale of the deployment. During deployment, installers will require special tools for measuring signal strength and propagation to ensure complete network coverage.

If your site already has WiFi infrastructure, you can use a high-level rule-of-thumb to determine your CBSD requirements. For indoor deployments one CBSD will typically supply the equivalent coverage of two to three WiFi Access Points. For outdoor deployments, one CBSD can replace from 12 to 20 WiFi Access Points depending on terrain and other factors.

Planning – Indoor/Outdoor, Use Cases, Spectrum Usage

You can now begin planning where to place your CBSDs. CBSDs have different power limits depending on their class: One watt for Category A devices (indoor or outdoor) and 50 watts for Category B devices (typically outdoor). As a general guideline, in a typical office environment a one-watt CBSD has an effective coverage area of about 10,000 square feet. For outdoor applications, a 50-watt CBSD has an average effective range of 1.5 – 2 miles using a 160-foot antenna. To avoid interference with any incumbents in the area using the same band, CBSDs may have to reduce their power levels. As a result, in practice the range of the CBSDs, particularly outdoors, may be reduced at certain times.

In addition to range considerations, you will need to estimate the number and types of devices that will connected to each CBSD. From there you can calculate your data bandwidth requirements. TDD LTE throughputs can be calculated depending on several parameters such as TDD configuration, channel bandwidth, Downlink and Uplink Modulation supported, as well as MIMO capability of the CBSD. See examples in the table below. The table lists peak rates shared across all connected users. You can use an online calculator (**https://www.cellmapper.net/4G-speed**) to determine the available bandwidth. As you get further away from the CBSD, total throughput will drop; we therefore recommend you design your RF footprint to maintain a cell edge that sustains 15/5Mbps DL/UL throughput. Unlike WiFi, your OnGo signal will remain consistent to the cell edge.

TDD Config (with: Normal Cyclic Prefix + Special Config0)	Channel Bandwidth	Modulation	MIMO	Peak DL	Peak UL
1	10	DL - 64 QAM	2x2	33.48Mbps	10.44Mbps
		UL - 16 QAM	4x4	66.96Mbps	10.44Mbps
1	20	DL - 64 QAM	2x2	66.96Mbps	20.88Mbps
		UL - 16 QAM	4x4	133.92Mbps	20.88Mbps
2	20	DL - 64 QAM	2x2	97.2Mbps	10.8Mbps
		UL - 16 QAM	4x4	194.4Mpbs	10.8Mbps
6	20	DL - 64 QAM	2x2	51.84Mbps	103.69Mbps
		UL - 16 QAM	4x4	25.92Mbps	25.92Mbps
6	20	DL - 256 QAM	2x2	69.12Mbps	38.88Mbps
		UL - 64 QAM	4x4	138.24Mbps	38.88Mbps
1	20+20 DL-CA	DL - 256 QAM	2x2	178.56Mbps	31.32Mbps
	20+20 UL-CA*	UL - 64 QAM	2x2	178.56Mbps	62.64Mbps

* In development now.

You should also note where the data streams are going. If your traffic is staying entirely within your private network, any connection to external networks will remain unaffected. However, if you intend to send multiple video streams to the Internet, your backhaul infrastructure will need sufficient capacity to handle the load.

Throughput needs of some various applications:

- 480p video (640x480) – 2.5 Mbps
- 720p video call (1280x720) – 3 Mbps (each way)
- 1080p HD video (1920x1080) – 8 Mbps
- 4k HD video – 20-25 Mbps
- Normal voice call – 12 kbps
- HD voice call – 50 kbps

Note: When a device is moving, its effective bandwidth demands increase. If this is the case, we recommend you add an additional 10% to your calculated bandwidth requirements for planning purposes.

Based on your total bandwidth needs, you can estimate the number of channels you will need. If your scenario needs more data than can be provided in a single channel, you can deploy multiple channels – either operating as a single 20 MHz channel, or using carrier aggregation to provide more throughput. The network can also allocate downlink and uplink data in different ratios, allocating for more (or less) uplink capacity.

PAL vs. GAA

In general, for most private indoor LTE deployments you should not require a PAL. However, you should consider investing in a PAL if your implementation meets one or more of the following criteria:

- Large area or outdoor deployment – If your implementation uses Category B CBSDs, or otherwise covers a large geographic area.

What is a PAL and do I Need One?

There are three tiers of access to the CBRS band:

- Tier 1: Incumbent users such as the federal government and fixed satellite users.
- Tier 2: Priority Access License (PAL) users—licensed wireless users who acquire spectrum through an auction. The SAS will ensure PAL users do not cause harmful interference to Tier 1 users and will protect PAL users from interference by General Authorized Access (GAA) users.
- Tier 3: GAA users who will deploy "lightly-licensed" devices. The SAS will ensure GAA users do not cause harmful interference to Tier 1 incumbents or Tier 2 PAL users.

Of the 15 CBRS channels, PALs are available for up to seven in the lower 100 MHz. Unused channels (and channels not being used by the incumbents) are available for GAA users. PAL users do not receive guaranteed access to a channel but are much less likely to be denied access by the SAS. If a PAL holder fails to use their allocated channel(s) for more than seven days, the SAS frees up those channels for GAA users.

Whether or not you need a PAL depends on a number of factors:

- The most important factor is how critical your network is to your operations. PAL holders are much less likely to be impacted by other users and can only be denied access when an incumbent user needs access to the channel.
- Are there a number of other CBRS networks in your area? If a number of other private GAA CBRS users exist in the same area, a PAL will help ensure that you receive preferential access.
- Does your network cover a large area? The larger your network, the more likely you will overlap with another CBRS network. A PAL will reduce chances of interference.

If you are unable to secure a PAL in the auction, you may be able to lease spectrum from an existing PAL holder. But given that PAL holders are not required to lease, it may not be possible to get a PAL in your area.

SAS operators can provide guidance on the availability of spectrum in your area.

- Mission-critical – A PAL gives your network higher priority, increasing the chances of spectrum access.
- Crowded environment – If you deploy your network in a very dense urban environment. As noted earlier, PAL users are afforded protection from GAA users.

The FCC auctions PALs on a per-county basis. Light-touch leasing rules allow for PALs to be sublicensed outside of areas where the PAL owner is broadcasting. PAL holders are not required to sublicense, however. More information on the PAL auction process can be found here: **https://www.fcc.gov/auction/105**.

Vendor Identification

As part of deploying your Private LTE network you will need to select many vendors. At the planning stage, you should begin to identify potential vendors. Once you reach the design stage you will need to choose your vendors.

SAS Vendors

The FCC has already approved several SAS vendors. While the essential functions of the SAS are defined by the FCC, each SAS vendor offers a variety of additional services, as well as a range of commercial terms. You can view a list of current SAS vendors here: **https://cbrs.wirelessinnovation.org/sas-administrators**.

Customer Premises Equipment and CPE-CBSDs

In the telecommunications world, the term "Customer Premises Equipment" (CPE) is widely used. Unfortunately, the exact definition of the term can often vary depending on the segment of the industry in question and the technology in use. In the OnGo context, the term CPE officially means an LTE UE operating in the CBRS band. However, the term is often applied to any non-mobile device that is part of an OnGo network, especially if the device does not face an end-user. This includes CBSDs. If you encounter the term CPE, be careful to clarify what is meant by the term.

There is also another type of CBSD called a CPE-CBSD. A CPE-CBSD can transmit at a higher total power level (>23dBm EIRP) than other end-user devices (EUDs) but can do so only after registering with the SAS. These devices are typically used in Fixed-Wireless Access (FWA) applications, as a CPE-CBSD must be non-mobile. Since they have a higher transmit power level, CPE-CBSDs can connect to a base station at a longer range than normal EUDs.

In an OnGo deployment, a CPE-CBSD can be an LTE UE (EUD) with the ability to connect to another CBSD over longer distances than other UEs. It may also include an eNB, allowing the CPE-CBSD to extend your coverage area when wired backhaul is impractical.

CBSD Vendors

Multiple CBSD vendors offer OnGo-certified devices. Differences between vendors include power levels, antennas, number of devices, throughput, and other configuration options. A full list can be found here: **https://www.cbrsalliance.org/certification/**.

Evolved Packet Core (EPC) Vendors

To function, CBSDs must connect to an Evolved Packet Core (EPC). The EPC provides mobile device management functions in the control plane and enables data packet exchanges between the mobile device and applications in the packet network on the data plane. You may deploy an EPC on-site, co-locate with the CBSDs, or use a cloud-based EPC service. CBSDs interoperate with the EPC; therefore, it is essential that you select a compatible EPC.

Element and Device Management System (EMS/DM) Vendors

The EMS and DM systems are tightly integrated with the CBSD and the EPC. The EMS typically provides control, configuration, management, and data collection services for the EPC; while the DM handles lifecycle management for the CBSD, including activation, configurations, and fault and performance management. The EMS/DM may be provided by the CBSD or EPC vendor, or by independent network management vendors that support the necessary management standards.

End-User Devices (EUDs)

Of course, critical to a private LTE deployment are the EUDs, also referred to as user equipment (UE), that will connect to your network. Any LTE UE device that supports Band 48 can connect to an OnGo network. Fortunately, many handsets on the market today already support Band 48.

If you have existing devices that you want to connect to your Private LTE network that do not support Band 48, you will need a bridging device. This can be a USB dongle or similar device that connects to an existing physical interface. If the device supports another wireless technology, the use of an OnGo EUD bridge in this manner can extend your Private LTE network to include multiple devices, effectively using OnGo as a backhaul connection.

The full list of certified devices can be found on the OnGo website: **https://www.cbrsalliance.org/certification/**.

SIM Provisioning

You will also need a system for provisioning SIMs. You can purchase either a dedicated UICC writer, or a software package for eSIMs. The type of SIM provisioning system you need is based on the EUDs that will connect to your network. SIM provisioning is typically part of an EMS/DM solution, but you may need to acquire this capability separately.

Certified Professional Installer

The FCC Part 96 rules that define CBRS generally require that CBSDs be registered with the SAS by a Certified Professional Installer (CPI). All Category B CBSDs, and any Category A CBSDs that are not able to self-geolocate, must be registered by a CPI. While CPIs are not required to install the CBSDs themselves, they are responsible for the accuracy of the registration data.

There are currently several training options for CPIs. A list of WInnForum-accredited Training Program Administrators (TPAs) can be found here: **https://cbrs.wirelessinnovation.org/cpi-program-administrator**.

Integrated Solution Vendors

As an alternative to contracting with individual vendors, multiple companies provide integrated solutions services. These vendors can take care of the details of planning, design, installation, and operations support. Many are members of the CBRS Alliance. A list of our members can be found here: **https://www.cbrsalliance.org/about-the-cbrs-alliance**.

Networking Plan

The primary consideration for IP networking is what type of physical network infrastructure your CBSDs will use to connect to each other and your internal network. Different CBSDs support different interfaces for their backhaul connections – Ethernet, optical fiber, or even wireless links. If your CBSDs use Ethernet for their backhaul,

your existing Ethernet infrastructure for your WiFi network may suffice for your OnGo deployment. If your deployment will use a large number of channels to support very high bandwidths, or your network infrastructure already carries significant traffic, you will need to make sure your backhaul connection has enough available bandwidth to support your needs. If not, you may need to add additional backhaul capacity.

You also need a backhaul connection if your system will interface with other networks (such as the public Internet). As with the internal network, you need to make sure that your total backhaul capacity can support the amount of data you will be carrying. Bandwidth is often set by contract, so make sure to check that you have sufficient bandwidth for all of your needs. Even if your network doesn't provide access to the Internet, the CBSDs and Domain Proxies must be able to connect to the SAS. We therefore recommend installing high-availability or redundant connections wherever possible, as your CBSDs will shut down if they are unable to periodically check in with a SAS.

Also bear in mind that your data needs may change over time and will likely increase. Rather than aiming for "just enough," we recommend building in plenty of headroom, particularly when it comes to your on-site infrastructure. You can increase backhaul bandwidth relatively quickly, but installing more cables is not a trivial effort. As a general rule, bandwidth demand rises 30% per year. We advise planning for twice your current needs to provide reasonable headroom for growth.

Security

Any network system must address security. Fortunately, OnGo has LTE security "baked-in" to the system, so achieving enterprise-level protection demands little to no extra work. If you require additional security, you should consider this in your selection of CBSDs and management systems.

Existing Data Infrastructure

When planning your OnGo deployment, you should consider any existing data infrastructure, particularly other wireless systems such as WiFi. OnGo excels at providing mobility, coverage in complex RF environments, and reliable, consistent

connectivity given a large number of connected devices. In a multi-network architecture, assigning devices (and their traffic) to the most appropriate network can improve the performance of the entire network. As a simple example, fixed devices can be placed on a WiFi (or wired ethernet) network, while mobile devices and devices in locations with poor WiFi connectivity can be assigned to the OnGo network.

Business Case

When deploying any new system, assessing both costs and benefits is an essential requirement. While the details differ with each system, keep in mind that once you have deployed a private LTE network to address a particular use case, the incremental cost to support additional use cases is much lower. In practice, the return on investment (ROI) for adding functionality often turns out to be significantly higher than that based on the initial use case.

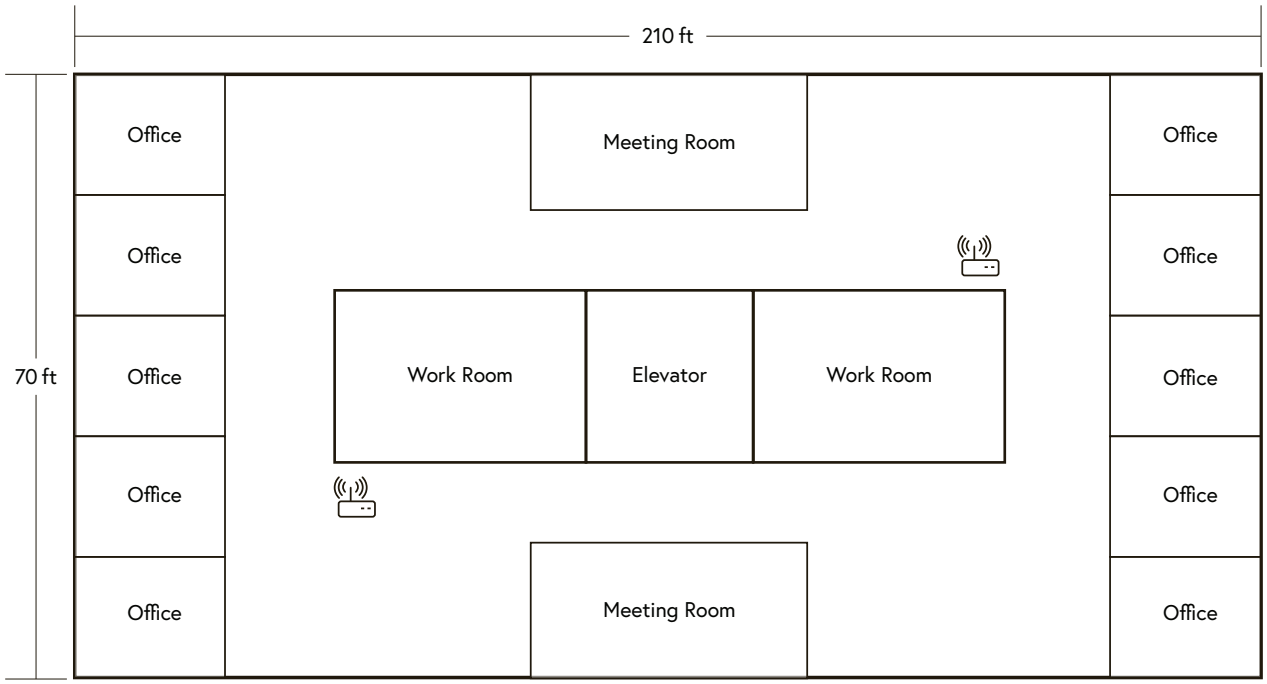
Scenario A: Smart-Building Network Planning

To provide a more specific example of the planning required for your network, we will illustrate with our first scenario: a smart office building.

The building stands eight stories tall, with dimensions of 70 by 210 feet. The structure is composed of reinforced concrete, with internal partitions of metal studs covered with drywall. Offices and conference rooms line the outer perimeter, with a central stack for the elevator and stairwell. Each floor has been wired for Ethernet, originating in the wiring closets adjacent to the elevator stack, and reaching into the offices and conference rooms. AC power is available throughout each floor.

Given the overall size of each floor, and the obstructions presented by the elevators and work rooms, it is determined that two CBSDs per floor will be needed. Spacing them sufficiently far apart will ensure full coverage.

Figure 3.



Each floor has 50–100 sensors and controls installed, including two high-definition security cameras. The security cameras generate the majority of traffic, with each one continuously sending 8 Mbps of uplink traffic. Given that the sensors and controls

generate only a few kbps total, this infrastructure traffic requires approximately 16 Mbps of uplink per floor. By attaching one camera to each CBSD, one channel will be able to meet these requirements with plenty of bandwidth to spare. If additional cameras are needed, a more uplink-heavy configuration can be used.

Since the deployment covers a relatively small area, and there aren't many other CBRS networks in the area, a PAL is likely unnecessary. However, if the network needs to support a complex of buildings, including outdoor spaces, a PAL may be required. Details from the site survey will help make that determination.

The building already has some wired data infrastructure to support the various tenants, with a shared server room on the ground floor. There is plenty of capacity on the building's ethernet system to support the CBSD, so no new infrastructure is needed.

Most of the traffic from the network will be remain internal; therefore, changes to the backhaul connection to the Internet will not be needed.

The EPC and network management system do not need to be full-featured. Device provisioning will happen infrequently, so the configuration of SIMs as well as the network can be done manually. None of the devices will be roaming to other networks, so agreements with other wireless network carriers are not needed.

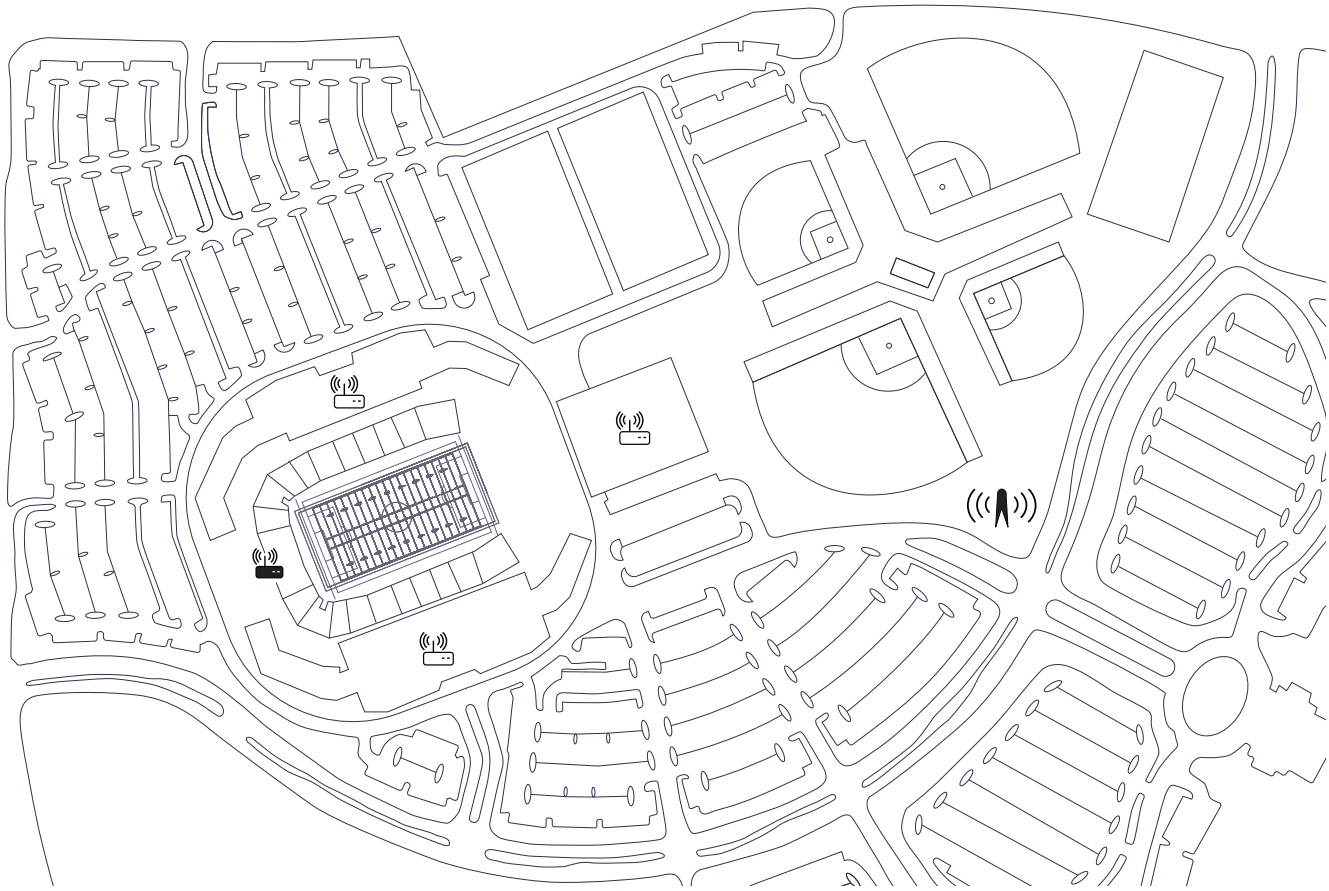
When it comes to selecting vendors, the critical consideration is getting a CBSD that can handle the number of device connections anticipated. Given that all CBSDs reside indoors, a high power (Category B) CBSD is not necessary.

Scenario B: Sports Venue Network Planning

Our second scenario, for a large sports and event venue, is significantly more complicated than a single building.

The site covers 72 acres and includes a main stadium, several other athletic fields, and single-level parking to support maximum usage. The main stadium area, built of reinforced concrete, contains locker rooms, offices, and a press box. The total seating capacity of the main stadium is 18,000. The stadium has some wired data infrastructure in the form of Ethernet feeds to the press boxes and offices. A high-definition video screen on the scoreboard has a direct HD video connection to the central controller in the press box, into which several other wired video feeds connect from various locations in the stadium. AC power is available inside the stadium and at the numerous lighting poles around the grounds. There is a small electronics closet in the press-box area for supporting the Audio-Video system that can also be used for any servers needed.

Figure 4.



Based on the site map, four Category A CBSDs will be needed: one in the stadium area, one in each of the two locker rooms, and one in the offices. With the parking area lights serving as a convenient mounting position, two outdoor (Category B) CBSDs will provide coverage to the larger grounds and the stadium area.

The device ecosystem consists of the personal phones and tablets of the site staff, the referees, coaches, and staff of the teams playing. The system should therefore support approximately 100 people, each using an average of 1.5 devices, for a total of 150 devices. Also, point-of-sale systems at the various concessions and ticket offices will add another 50 devices. Three mobile HD cameras also require support, with the desire to simultaneously provide live video from all three cameras as they move around the playing area. Based mainly on the number of video feeds needed (three 8Mbps links), that area of the network will need to be uplink heavy, supporting two channels with carrier aggregation to accommodate future growth.

Because of the dense suburban location of the site, the bandwidth need to support the video cameras, and the need for a large amount of outdoor coverage, four channels will be needed. Given these factors, a PAL to ensure channel access will be required.

Devices will regularly move throughout the stadium complex, so the network must support full mobility among the CBSDs within the entire complex.

The system must provide seamless connectivity for authorized devices, giving them full access to voice and data. Therefore, mobility into and out of the network must be supported, which will necessitate roaming agreements with other network carriers.

Given frequent staff changes and the need to accommodate visiting teams, the system must support the ability to add and remove devices easily from the list of authorized devices.

After defining the network capabilities needed for your private LTE deployment, surveying your location, and selecting vendors, the next step is identifying the network elements best suited for delivering them. These network elements include endpoint devices, a radio system and Access Points, and core network services.

Vendor Selection

SAS Selection

Now is the stage where you will need to contract with one of the SAS operators to provide service for your deployment. Different SAS operators will offer a variety of commercial and contract terms (per CBSD, flat fee, etc.), and you will need to select the one that best supports your deployment. Your choice of SAS vendor will depend on many factors, including:

- Commercial terms for interfacing with the SAS.
- Additional services provided by the SAS, such as spectrum planning and area information.
- Does the SAS vendor have ESC sensors deployed for your area?
- Need for a Domain Proxy (see below).

CBSD Selection

Now you are ready to select the CBSDs. The general Key Performance Indicators (KPIs) that you should consider when choosing a vendor include:

- Indoor and outdoor CBSD options.
- Supported power levels.
  - Category A devices can transmit up to one watt of power, but many vendors offer options with lower power levels.
- The number of devices each CBSD can support.
- Uplink/downlink configuration support.
- Need for a CPI (see below).
- Carrier aggregation support (uplink and downlink) if bandwidth needs require more than one channel.

- Lifecycle management capabilities (activation, provisioning, operating, monitoring).
- Backhaul options.
- Ability to support multiple-location deployments in a single platform.
- Flexibility of adding new CBSD devices from different vendors.
- Integration capability with existing Fault/Performance Management and other systems.

EPC Selection

A basic EPC consists of four main network elements: MME, HSS, SGW and PGW. Other EPC network elements may or may not be needed, depending on your deployment needs. The Mobility Management Entity (MME) and Home Subscriber Server (HSS) provide mobility and device access controls. The Serving Gateway (SGW) and Packet Gateway (PGW) are the network elements providing actual bearer data transport for mobile devices by routing data packets between CBSDs, your local network, and any connected networks such as the public Internet. The different elements of the EPC can be run on separate devices or integrated into a single device.

EPC network elements can be deployed entirely in the cloud, on-premise together with CBSDs, or in a hybrid mode. Which architecture you select depends on the needs of your deployment, available backhaul, and cost considerations. Likewise, your deployment needs (such as seamless roaming to/from the public networks, network slicing, etc.) dictate the features your EPC will need to support. EPC providers can provide a range of solutions based on your needs. They often offer different management system capabilities as well, which we will discuss below.

Element Management System (EMS)/ Device Management (DM) Selection

An EMS/DM can be located on the premise or in the cloud. It can also reside side-by-side with the EPC and perform EPC and Device (CBSD) management functions. Key considerations include:

- Standards support (SNMP, TR-069, NetConf, etc.).
- Simplified dashboards of overall status, key performance indicators, and alarms.

- CBSD Device Management capabilities to enable ease of device deployment and ongoing management.
- Data Analytics and reporting of Key Performance Indicators (KPIs) and other performance metrics.
- Fault Management and Alarming.
- Troubleshooting and diagnostic support.
- Redundancy and Resiliency.
- Ability to support multiple-location deployments in a single platform.
- Flexibility of adding new CBSD devices from different vendors.
- Integration capability with existing Fault/Performance Management and other systems.

Do I Need a CPI?

For some OnGo deployments, you may not need a CPI. You should be able to skip having a CPI involved if all of the following are true:

- All of your CBSDs are Class A (< one watt).
- All of your CBSD antennas are less than 6 meters in Height Above Average Terrain.
- All of your CBSDs include the capability to automatically determine their location.
- You aren't using a PAL.

CPI Selection

You will also want to select a CPI at this time. Key considerations include payment terms and additional services the CPI can provide.

Note: Some Category A CBSDs have an autosensing function that can detect their location using GPS/GNSS and do not require a CPI to register their configuration with the SAS.

CBSD Configuration

The primary element of an OnGo deployment is the CBSDs – the devices your end users will connect to. Depending on your implementation, you may need one or many. Exactly how many, where they need to be placed, and how they will be sectored, are functions of the detailed geometry of your site. Key aspects to consider at this stage include:

CBSD Placement and Sectorization

CBSDs and their antennas need to be placed where they can provide optimum coverage of the devices that will be using your system with the minimum number of CBSDs. If the area to be covered is large or contains lots of obstructions (walls, trees, and

other obstacles), detailed signal measurements and pattern maps may be needed to determine the required coverage.

CBSD Configuration

In addition to determining the placement of your CBSDs, they also need to be configured to support your deployment. You can configure your network to provide more uplink or downlink capacity depending on the kind of data traffic the system needs. CBSDs can be sectorized as well – segmenting their coverage area into different sectors operating in parallel.

Existing CBRS Networks/Incumbents

The presence or absence of other CBRS networks in the area can affect your deployment. The selected SAS may be able to provide this information, or use a spectrum analyzer or similar equipment to determine potential interference in the area.

Detail the Spectrum Requirements to SAS Vendor

The SASs need to know how many channels your deployment will consume. They can also provide guidance on the location of any nearby incumbents, availability of channels, and any likely power restrictions in your area.

Multiple companies provide services supporting the configuration of private LTE deployments. These services include mapping of the RF environment, checking propagation via modelling and direct measurement, and more. With this support you can be assured of optimum coverage.

Network Design

At this stage, you need to decide on the design of the network infrastructure supporting your Private LTE network. Here are a number of important topics for you to consider:

Domain Proxies

CBSDs can be grouped behind a Domain Proxy service that communicates with the SAS. The Domain Proxy aggregates all communications from the CBSDs and provides a single interface point from the SAS to the CBSDs. This can reduce your configuration and registration complexity, particularly if you have a high number of CBSDs. Whether

or not a Domain Proxy is needed depends on the capabilities of the selected CBSDs, as well as the terms offered by your selected SAS vendor. The Domain Proxies are CBSD-vendor specific, so if you have CBSDs from multiple vendors, you will need a Domain Proxy element for each vendor.

OnGo, LTE, and 5G

OnGo is currently LTE in the CBRS band. However, in the next release we will add 5G NR support. 5G will bring improved data rates, reduced latency, greater device density, and new network management features – including advanced network slicing options – to OnGo deployments.

Network slicing

You can configure your Private LTE network to provide multiple independent virtual networks, each with different configurations, controls, and features. For example, a network can be sliced to allow staff to have access to your internal network and voice calls, while guest users can access only the public Internet.

Note: While LTE supports basic network slicing, more advanced capabilities are supported by 5G.

EPC

LTE networks require core network services to manage devices, enable mobility, and support voice, video, data, and application services. EPC solutions can be physically deployed on-premises, contracted as a service, accessed via the cloud, or delivered as a hybrid solution. Because OnGo private LTE deployments are so flexible, organizations can choose to purchase or subscribe to core services for the solution that best fits their technical and budget requirements. See CBRSA-TS-1002 for details on possible core network configurations.

Neutral Host Networks

A CBRS deployment can be configured to function as a Neutral Host Network (NHN). In this configuration, the CBRS network extends the networks of multiple Major Network Operators (MNOs). Subscribers to the supported MNOs are given access to the CBRS network transparently, so that it appears as their home network. They can then roam into and out of the CBRS network completely seamlessly.

This functionality requires special configuration of the CBRS Network and agreements with the MNOs. A separate guide will provide additional details.

The same EPC used for a private LTE network can also enable additional expandability, allowing organizations to move mobile devices seamlessly from private to public connectivity via OnGo. For example, assuming you establish roaming relationships between your OnGo private LTE network and the public

LTE mobile network operators (MNOs), users can roam from public networks to OnGo private LTE networks, or from OnGo private LTE networks to public networks.

EPCs can even interoperate with other bands and technologies to provide connectivity failover, expand capacity, and eventually accommodate 5G-based technologies. OnGo ecosystem service providers, system integrators, and vendors can help organizations find the optimal solution for each deployment.

Do I Need to Reserve ID Numbers?

In order to prevent potential interference issues with other LTE networks in your area we generally recommend you reserve ID numbers. However, if your system is physically isolated from other LTE networks, and devices are not going to be moving in and out of your coverage area, then you can probably get by without ID numbers. That said, it is generally a good idea to get them anyway, as you may require ID numbers in the future as new services are added or outside circumstances change.

Roaming Agreements

If your use case requires seamless roaming onto the public mobile networks, you will need to execute roaming agreements with the mobile network operators (MNOs). In addition to the commercial terms, the EPC will need to be configured to support such roaming. Depending on your use case you may need to set up a roaming agreement with just a single MNO (e.g., if the mobile devices all use the same MNO for service) or with multiple MNOs (e.g., in a BYOD environment). See our forthcoming Neutral Host Networks deployment guide for additional details on this capability.

Identifiers

You will need to acquire several unique identifiers from the CBRSA in order to ensure that your private LTE deployment interconnects correctly with (and does not interfere with) other LTE networks.

CBRS Private LTE networks typically use a shared Home Network Identifier (SHNI) (e.g., CBRSA's 315-010). This can potentially cause problems, as the various globally unique identifiers used in LTE (GUMMEI, etc.) may not actually be unique when multiple private LTE networks are deployed. Therefore, your deployment will require several unique identifier numbers for your implementation to ensure proper operation.

The following identifiers can be acquired from the CBRS Alliance:

- A single CBRS-NID (Network Identifier). This number, when combined with the SHNI, provides a truly unique identifier for your network.
- A single MME Group ID (MMEGI).
- One Macro eNB ID for each CBSD in your deployment.

These numbers can be obtained from the CBRS Alliance. An online system is planned, but until that system is deployed, please contact **SHNI@cbrsalliance.org** to acquire the needed identifiers.

If your network is isolated from other CBRS networks, and devices will be used only with your network, you can use the CBRS SHNI, and whatever arbitrary values for the CBRS-NID, MMEGI, and eNB IDs you desire. However, you should take precautions to ensure that the values you use do not match those of any other CBRS networks in the immediate area.

You may also acquire a dedicated global unique Home Network Identifier from the ITU, or request a different Shared HNI from other sources, but this process can be significantly more complicated than getting identifiers from the CBRSA.

In either case, you will need to make sure that the Tracking Area Identifiers (TAIs) used by your system are unique. If you do not, devices may be unable to connect to your network, specifically if the TAI is the same on a neighboring network. We recommend using your IMSI Block Number (IBN – see below) for the Tracking Area Code (TAC) element of the TAI. If you need additional TACs for large deployments with lots of CBSDs, we recommend you add 10,000 to the value of the previously used TAC (i.e. IBN + 10,000, IBN + 20,000, etc.). This method is not guaranteed to create a unique number, but it should be sufficiently unique to prevent collisions.

IMSI Block Numbers

If your network is using devices that connect only to your system, you will need to obtain an IMSI Block Number (IBN), which can be assigned by the US IMSI Administrator (**https://imsiadmin.com/imsi-home**). If you are going to have more than 100,000 devices, you will need an additional IBN. This IBN can be used to generate IMSI numbers to be assigned to a device's SIM card or an equivalent system such as an eSIM.

Backhaul

This is also the time to make sure any additional network infrastructure you will need is in place. This includes providing power as well as IP connectivity to the CBSD sites and ensuring that the CBSDs will have the bandwidth needed to connect to other networks, including the Internet.

End-User Devices (EUDs)

End-User Devices (EUDs) are what connect to your private LTE network. Devices can include mobile phones, tablets, laptops, IoT devices, internal communication systems or applications, modems, cameras, gateways, or routers to other networks and systems. Because OnGo uses LTE as its foundational technology, industry standards exist for security, interoperability, and service provision.

Many existing LTE devices already support OnGo. As long as the chipset used in the device supports the 3.5GHz CBRS band (Band 48), the device can use OnGo. In many cases, existing equipment can be converted to the OnGo network without replacement, although some devices may need software updates from operators to enable the CBRS band. You can see the list of OnGo certified EUDs at: **https://www.cbrsalliance.org/certification/**.

About LTE Identifiers and OnGo

In LTE, networks are identified using a five or six digit code, called the Public Land Mobile Network Identifier (PLMN-ID), that consists of a three-digit country code, and a two or three-digit Mobile Network Code. This information is broadcast by the LTE base stations (also called Evolved Node Bs, or eNBs). Devices then compare that PLMN-ID to the Home Network Identifier (HNI) stored in their SIMs to determine if it is part of their home network. eNBs can also broadcast a 27-bit Closed Subscriber Group Identifier (CSG-ID) that allows only devices with that ID in their SIM to connect with the designated eNBs.

Since there aren't that many PLMN-IDs, the CBRS Alliance has obtained a single shared PLMN-ID for use by OnGo networks as their HNI (315-010). We have repurposed the CSG-ID as the CBRS-NID to allow devices to identify individual OnGo networks.

Not all EUDs support the CSG-ID mechanism. In this case the EUDs will attempt to connect to any network using the OnGo shared HNI. When the device attempts to connect to a network using the OnGo shared HNI, an unrecognized device will be denied access, at which point it will attempt to connect to the next available network. This means EUDs that don't support the CSG-ID may take longer to connect to the correct network.

Some important considerations when selecting EUDs:

- Does it need to be a consumer-grade or an industrial-grade device?
- Does it support other bands than CBRS?
- Does it support the bandwidth and power levels needed for your deployment?
- Does it support the carrier aggregation configuration of your network?
- Does it support the physical and wireless interfaces you need?
- What kind of SIM does it use? Does it support Dual-SIM operation?

IMSIs and SIMS

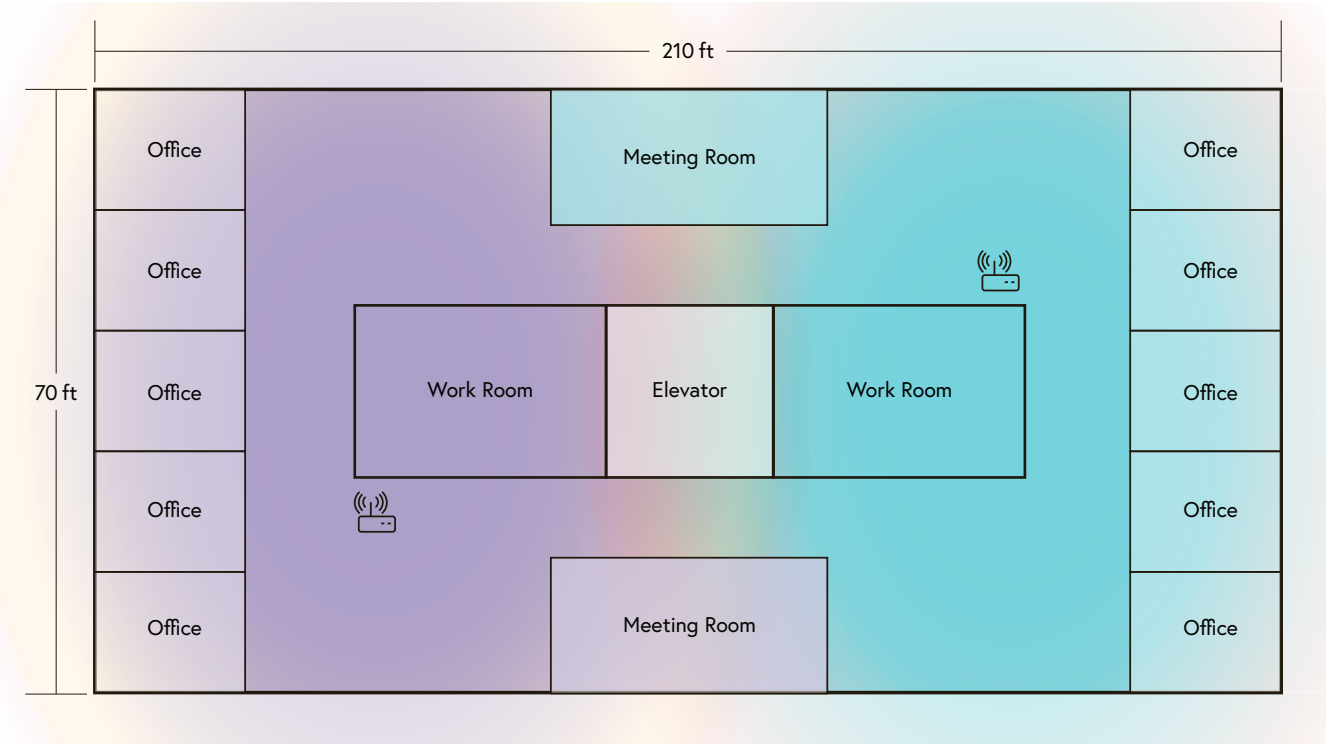
Related to the LTE identifiers are International Mobile Subscriber Identity (IMSI) Block Numbers. An IMSI is a unique identifier that is used to identify devices. The IMSI is what is placed in the Subscriber Identity Module (SIM), either on a physical Universal Integrated Circuit Card (UICC, commonly called a "SIM Card") or as an Embedded-SIM (eSIM). Some devices support multiple SIMs in a single device.

Scenario A: Smart-Building Design

At this point a set of vendors has been selected. A single vendor will provide the CBSDs, EPC, Domain Proxy, and EMS as an integrated solution, making the system easier to configure and maintain. The SAS vendor has been selected as well, with commercial terms based on the Domain Proxy aggregating the CBSD communications. Since the CBSDs on the upper floors are going to be higher than 6 meters off the ground, a CPI is needed.

A specialist has been contracted to check that the desired locations of the CBSDs will provide complete coverage, especially for the security cameras on the perimeter of the building. Based on the detailed measurements, the contractor will recommend where to place the CBSDs and how to configure their antennas best. Two CBSDs will cover each floor.

Figure 5.



The EPC will be located on the site, in a network closet, and will run on a single server along with the Domain Proxy and EMS elements.

While roaming into and out of the public networks is not a requirement, a set of identifiers will need to be reserved to ensure that there are no interoperability problems given that additional networks are deployed in the area. A CBRS-NID and MMEGI, as well as Macro eNB IDs for each CBSD, will need to be reserved.

Scenario B: Sports Venue Design

Vendors are now selected. In this case, two CBSD vendors will be used: one for the indoor Category A CBSDs, and another for the outdoor Category B CBSDs. The chosen EPC is compatible with both CBSD vendors, and also supplies the EMS element. Two different domain proxies are needed, one for each CBSD vendor. The SAS vendor has also been selected, with the commercial terms based on the Domain Proxies aggregating the CBSD communications.

A specialist service provider has prepared a detailed map of the coverage area to determine the ideal placement of the CBSDs. Two Category B CBSDs will be needed to ensure proper coverage of the stadium area and the parking lots. The Category B CBSD in the stadium will provide coverage of the playing area and stands. It will also be the primary link for the HD video cameras, and will use two 10-MHz channels, in an uplink-heavy configuration, to provide plenty of capacity. Due to interior obstructions, three additional CBSDs will be installed to provide coverage for the offices and indoor training facilities.

To obtain the required PAL, PAL owners in the area have been contacted to discuss sublicensing terms. Also, given that several of the CBSDs are Category B devices, a CPI has been engaged to register the installations.

The EPC will reside on site in the AV closet, and will also host a domain proxy service.

Since users will be roaming into and out of the public networks, the full set of identifiers will be needed: a CBRS-NID and MMEGI, as well as Macro eNB IDs for each CBSD. Roaming Agreements with each of the Major Network Operators (MNOs) have been signed.

Figure 6.

Now it is time to start installing your CBSDs, EPCs, and the other equipment in your deployment.

CPI Requirements

All Category B CBSDs must be inspected and registered by a CPI. Some Category A CBSDs can determine their location automatically via GPS/GNSS and therefore do not always require a CPI. The most critical pieces of information that the CPI provides are the GPS coordinates of the CBSD, the power level, and the environment of the CBSD (indoor or outdoor).

You can find more information on CPIs at the WInnForum website: **https://cbrs.wirelessinnovation.org/cpi-program-administrator**.

PAL Configuration

If you have a PAL, or are sub-licensing from a PAL holder, the SAS needs to be provided with information about the CBSDs your network is using, so that they can be added to the list of CBSDs associated with the PAL.

SIM Configuration and Provisioning

Devices that will connect exclusively to your network must be provisioned with SIM cards configured specifically for your network, with a custom IMSI (using your IBN). For physical SIM cards, you will need to acquire SIM cards in the appropriate form factor, a SIM writer, and the necessary software. Devices with eSIMs can be provisioned using software, which is typically provided by the device manufacturer.

To properly configure your SIMs for connection to your network, you must set the Home Network Identifier (HNI) in the SIM to the Public Land Mobile Network Identity (PLMN-ID) of your network. For most Private LTE deployments using identifiers assigned by the CBRS Alliance, this is the CBRS Alliance's Shared HNI (315-010). Your specific network is identified by the CBRS-NID, which is provided in the SIM's Closed Subscriber Group (CSG) Identity field.

If you are building a standalone network and have not established agreements with any major network operators but want to support your users' personal devices on the system, you will need to provision those devices for dual-network support. This requires

that your users have dual-SIM capable devices, and you configure the secondary SIM to connect to your network.

In either case, you will need to register the device with your network services to allow access for the device. The details of how to do this differ by system, but generally involve entering the IMSI or IMEI identification numbers into the management system.

Spectrum License

If you have a PAL, the PAL holder will need to inform the SAS about the CBSDs that are being added to that PAL. If you do not have a PAL, and are instead using GAA for access, then no additional configuration information is required. Each CBSD in your system can only do either GAA or PAL.

EPC Configuration

At this time, your network's EPC element needs to be deployed and configured correctly to support your deployment. In particular, the system must be configured with the identifiers for your network (SHNI, CBRS-NID, etc.), and to work with your CBSDs.

Commissioning the CBSDs

Once installed, and with the configuration information (location, power level, etc.) recorded by the CPI, the CBSDs can be activated. The CBSDs will connect with the SAS and request channel access. In most cases, particularly if there are no incumbents in the area, the SAS will grant access to your requested spectrum in near real-time. However, if you are near an incumbent, or in an area with possible incumbent activity (most commonly on the coasts), spectrum authorization can take up to 48 hours.

Commissioning of End Devices

Once the CBSDs are activated, and channel access granted by the SAS, it is time to start connecting your devices to the network. For many devices, it's merely a matter of using a properly configured SIM, turning on the device, and waiting for it to find your network. Others may require manual connection.

Scenario A: Smart-Building Installation

The CBSDs are installed, and use their autosensing capabilities to register their location with the SAS. As a result, a CPI is not required.

The Domain Proxy, EPC and EMS are installed and configured by the vendor. The vendor has also provided a set of SIMs for use in the devices, pre-configured so that the devices may connect to the OnGo network.

Once everything is provisioned, the OnGo network is commissioned. After a few minutes, the CBSDs will be activated by the SAS. Once the system is active, client devices may be turned on and will connect automatically with the CBSDs.

Scenario B: Sports Venue Installation

The CBSDs have been installed, and the CPI has registered their information – along with the information on the sublicensed PAL – with the contracted SAS.

The Domain Proxy, EPC, and EMS have also been installed and configured by their respective vendors. The vendor has provided a set of SIMs for use in the devices connected to the network. The EMS is used to register the device information for the staff's personal devices to allow them to connect to the system.

Once provisioning is complete, the OnGo network is commissioned. The CBSDs are activated by the SAS after several minutes, though it may take up to 48 hours in some circumstances.

Like any system, a private LTE deployment requires support. If there is a problem, it is essential to remember the system's elements that will most likely be the cause. Here are some recommendations for critical things to remember:

Network Operations Center (NOC) Support

A private LTE deployment has an EPC back-end system: the access network that includes CBSDs and end devices as well as the transport between EPC, access, and end devices. All these components require operational support from a Network Operations Center (NOC). The EPC may be located on your premises, at an external site, or even be cloud-based. Faults in individual CBSDs or end devices may affect specific areas of the net. But if there is a problem with the EPC, the performance of the entire private network can be impacted. It is crucial to have a NOC monitoring the system 24x7, particularly when mission-critical applications are running on the network.

HW/SW Alarms

Individual CBSDs, the EPC, or end devices can develop hardware or software faults. These components generate an alarm when an error occurs and alert the NOC support team.

SAS Connectivity

If connectivity to the SAS is lost, the CBSDs will shut down after just a few minutes. This is why we recommend high-availability or redundant communications. If connectivity is lost, the SAS retains the grant for your network for seven days. As long as the link is restored within the specified timeframe, your network can resume operation immediately.

Channel Access

If an incumbent system becomes active, the SAS may direct your CBSDs to reduce power, or even shut down entirely.

Service Level Agreements (SLAs)

To ensure that your network operates at the needed level, you should establish Service Level Agreements (SLAs) with your vendors. The level of service guaranteed depends on how mission-critical your system is.

Key Performance Indicators (KPIs)

There are a number of pre-defined LTE-related KPIs that may be used to meet SLAs. Some include:

- Availability – Used to measure the percentage of time the network is available for users to make full use of the offered services.
- Retainability – Used to measure how often the users lose connectivity to the network typically due to poor coverage and quality.
- Integrity – Used to measure the character of the network through metrics such as throughput and latency.
- Mobility – Used to measure the network's performance while the users move through the coverage area of the system.
- Utilization – Used to measure the capacity of the network.

The source for the metrics for KPIs may come from the EMS of the CBSD vendor, or from the EPC. KPIs can also be custom-designed for specific use cases.

Monitoring

A network monitoring system plays a vital role in any private LTE deployment. This system should evaluate key performance metrics continually against your service level agreements (uptime, average throughput, etc.) and provide immediate notification of any problems that could impact critical services.

Priority Access License (PAL)

If system performance does not meet the desired level due to channel access limitations, you should consider acquiring or sublicensing a PAL.

Requirements Gathering

What is the purpose of your private LTE network?
Who will be connecting to your private LTE network?
What devices will be connecting to your private LTE network? How many of each? What SIM system do they use?
Which devices will be mobile within your network? Which devices will move into and out of your network?

Survey & Planning

Sketch of coverage area. Note locations of key devices, existing WiFi Access Points, power outlets, and data access.
How much data capacity do you need?

Traffic	Bandwidth	Number of Devices	Total Bandwidth
480p video	2.5 Mbps		
720p video	3 Mbps		
1080p video	8 Mbps		
4k HD video	20-25 Mbps		
Voice	12 kbps		
HD Voice	50 kbps		
Total			

Is a PAL Needed?
SAS, CBSD and EUD Vendors

Design

Selected SAS Vendor:	
Selected CBSDs:	
Number of CBSDs:	
Selected EPC:	
Selected EMS/DM:	
Selected CPI:	
Assigned CBRS NID:	(**SHNI@cbrsalliance.org**)
Assigned MME Group ID (MMEGI):	
Assigned Macro eNB IDs (one per CBSD):	
Assigned IMSI Block Numbers (one per 100,000 devices):	(**https://imsiadmin.com/imsi-home**)
SIM Provisioning Option:	
PAL License:	

Checklist

Install Checklist

Install and Configure CBSDs:
Install and Configure EPC:
CPI Registered With SAS:
SIMs Provisioned:
Commission CBSDs:
Commission End Devices:

Maintain & Service Assurance

KPIs:
Defined Alarms:
Internal Contacts (for alarms):
Operations Contact:
CBSD Support Contact:
EPC Support Contact:

Glossary

Term	Definition
AC	Alternating Current.
AP	Access Point: the WiFi equivalent of an eNB.
Backhaul	Connection from a network node (CBSD) other nodes and external networks.
BTS-CBSD	Base Transceiver Station CBSD: Fixed CBSD base station connecting to EUDs or CPE-CBSDs.
BYOD	Bring Your Own Device.
CBRS	Citizens Broadband Radio Service.
CBRS-NID	CBRS Network ID: a CSG-ID that identifies the provider of a network.
CBSD	Citizens Broadband Radio Service Device: Fixed Stations, or networks of such stations, that operate on a Priority Access or General Authorized Access basis in the Citizens Broadband Radio Service consistent with Title 47 CFR Part 96.
Category A	<30 dBm/10 MHz (<1 Watt/10 MHz) transmit power CBSD.
Category B	<47 dBm/10 MHz (<50 Watt/10 MHz) transmit power CBSD.
CPE	Customer Premises Equipment.
CPE-CBSD	A fixed device that communicates with a SAS via a BTS-CBSD and can exceed the EUD transmit power limit. In an OnGo context, it functions as a non-mobile UE.
CPI	Certified Professional Installer: an individual authorized by the WInnForum to register information about a CBSD with the SAS.
CSG-ID	Closed Subscriber Group Identifier.
DL	Downlink.
DM	Device Management System (for CBSD).
eNode-B	Evolved Node-B, an LTE base-station.
EIRP	Effective Isotropic Radiated Power: the transmitted power level of a wireless device.
EMS	Element Management System.
EPC	Evolved Packet Core: provides network services to mobile devices in LTE.
ESC	Environmental Sensing Capability.
eSIM	Embedded SIM: a SIM system without a removable UICC/SIM card.
EUD	End-User Device: an LTE UE in OnGo (e.g. a smartphone, sensor, etc.). Can be a fixed or mobile device. Transmit power level must be <23 dBm EIRP.

Glossary

Term	Definition
FCC	Federal Communications Commission.
FWA	Fixed-Wireless Access: A wireless telecommunication system where the devices are non-mobile. Often used for providing backhaul for other services.
GAA	General Authorized Access.
GHz	Gigahertz.
GTP	GPRS Tunneling Protocol: a tunneling protocol for managing mobile bearer data between an SGW and a PGW in an EPC.
HAAT	Height Above Average Terrain
HD	High Definition.
HNI	Home Network Identifier: the PLMN-ID of a device's home network.
HSS	Home Subscriber Server: the network element of an EPC, contains user-related and subscription-related information in a centralized database.
IBN	IMSI Block Number: a block of numbers granted for use by a network operator.
IMEI	Individual Mobile Equipment Identity.
IMSI	Individual Mobile Subscriber Identity.
IT	Information Technology.
ITU	International Telecommunications Union.
IoT	Internet of Things.
Kbps	Kilobits per second.
KPI	Key Performance Indicator.
LTE	Long Term Evolution: the 4th generation mobile technology; used in OnGo.
LTE UE	LTE User Equipment: a device (mobile or fixed) used by an end-user to communicate (e.g. a smartphone).
Mbps	Megabits per second.
MHz	Megahertz.
MIMO	Multiple-Input and Multiple-Output: a method for multiplying the capacity of a radio link using multiple transmission and receiving antennas to exploit multipath propagation.
MME	Mobility Management Entity: the network element of an EPC that controls mobile device access to the EPC.

Glossary

Term	Definition
MMEGI	MME Group ID that identifies a pool of MMEs.
MNO	Mobile Network Operator.
NHN	Neutral Host Network: an LTE network that provides coverage to multiple MNOs.
NOC	Network Operations Center: OnGo LTE in the CBRS band.
PAL	Priority Access License.
PGW	Packet Data Network Gateway: a network element of an EPC that provides connectivity from a UE to external packet data networks by being the point of exit and entry of traffic for UEs.
PLMN-ID	Public Land Mobile Network Identity: RAN Radio Access Network.
RF	Radio Frequency.
SAS	Spectrum Access System: manages and assigns CBRS spectrum use on a dynamic, as-needed basis across PAL and GAA users.
SGW	Serving Gateway: a network element of an EPC that routes and forwards user data packets to a PGW via GTP sessions, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers.
SHNI	Shared Home Network Identifier: a common PLMN-ID for use by OnGo systems (315-010).
SIM	Subscriber Identifier Module.
SLA	Service Level Agreement.
SNMP	Simple Network Management Protocol.
TAC	Tracking Area Code, part of the TAI.
TAI	Tracking Area Identifier.
UE	User Equipment: a device using the mobile network.
UICC	Universal Integrated Circuit Card: a SIM card.
UL	Uplink.
USB	Universal Serial Bus.
WInnForum	Organization that develops the standards for CBRS system elements to include the SAS, ESCs, CBSDs and CPI certification

About the CBRS Alliance

The CBRS Alliance believes that LTE-based solutions in the 3.5 GHz band, utilizing shared spectrum, can enable both in-building and outdoor coverage and capacity expansion at massive scale. In order to maximize the full potential of spectrum sharing, the CBRS Alliance enables a robust ecosystem through the management of the OnGo brand, and the OnGo Certification Program. For more information, please visit **www.cbrsalliance.org** and learn more about the expanded business opportunities OnGo is enabling.